PRIVACY IMPACT ASSESSMENT (PIA)

For the

DoD Unified Communications Enterprise Directory Service (UC EDS)
Defense Information Systems Agency (DISA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 3200
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier K890.14 - Identity Synchronization Service (IdSS)

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

The following authority allows DoD Unified Communications Enterprise Directory Service (UC EDS) to collect PII data:

- 5 U.S.C. 301, Departmental Regulation;
- 10 U.S.C. chapter 8; DoD Directive 5105.19, Defense Information Systems Agency (DISA);
- DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program;
- DoD Enterprise User Data Management Plan for Persons and Personas, August 11, 2010;
- Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS), March 11, 2009.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The Unified Communications (UC) Enterprise Directory Service (EDS) provides the capability to search for and display contact information for DoD personnel. The contact information is displayed in order to facilitate business communications with the contact. An example is to look up the business phone number for a DoD co-worker and then initiate a phone call to that DoD co-worker. Another example is to look up the business Instant Messaging (IM)/chat address for a DoD coworker and initiate an IM/chat session with that DoD co-worker.

The UC EDS does not collect PII directly from an individual nor does the UC EDS add any new or unique PII to any DoD system. Rather, the UC EDS obtains search results and data elements from other existing DoD systems that are already approved to collect, store, and disseminate PII. Specifically, the UC EDS retrieves contact data from the IdSS covered in the associated SORN K890.14. The UC EDS then displays search results and contact data to users. The contact data that the UC EDS displays is used to establish business communications (voice, video, IM/chat, collaboration, and email) with the contact. Accordingly, the UC EDS displays contact information such as name, business telephone number, business IM/chat/collaboration address, business video address, and business email address. Aside from name, this data is generally considered to be non-sensitive PII.

Use of the UC EDS, and therefore the ability to view UC EDS search results, is restricted to authorized and authenticated DoD personnel that access the UC EDS via secure SIPR transport.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risk associated with the UC EDS is that an individual's name and contact data are displayed in search results. This risk is addressed in the following ways:
- The risk is inherently minimal due to the type and limited amount of PII that is revealed. Aside from name, the contact data displayed in UC EDS search results is business related (e.g., business phone number) and is generally considered to be non-sensitive PII.
- The contact data displayed in UC EDS search results is already available for viewing in existing and approved systems such as the DoD Enterprise Email (DEE) Global Address List (GAL) and the whitepages.mil portal. The set of users for these existing systems is larger than and includes potential UC EDS users. Hence, display of this data to UC EDS users does not increase the breadth or depth of disclosure of this data beyond what is already approved.
- Access to the UC EDS is restricted to DoD subscribers that are authorized by their DoD organization to make use of UC communications systems/services. In addition, these DoD subscribers are authenticated when accessing those UC communications systems/services.
- Transport of UC EDS search results is via SIPR infrastructure and is secured with various technical mechanisms (e.g., encrypted connections, firewalls, VPN).

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. All DISA organizations can, at their discretion, subscribe specific personnel to UC communication services that display UC EDS search results. Such authorized subscribers will be able to view UC EDS search results. The UC EDS is employed within the following DISA provided UC communication

systems/services: Avaya Enterprise Session Controller (ESC), and Cisco ESC

☒ **Other DoD Components.**

Specify. All DoD components can, at their discretion, subscribe specific personnel to UC communication services that display UC EDS search results. Such authorized subscribers will be able to view UC EDS search results. The UC EDS is employed within the same DISA systems as noted above.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. All DoD components can, at their discretion, subscribe specific DoD contractors to UC communication services that display UC EDS search results. Such authorized subscribers will be able to view UC EDS search results. The UC EDS is employed within the same DISA systems as noted above.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

Display of contact data is required to implement and operate DoD communication systems. Contact data is made available so that individuals can communicate with each other in the variety of modes that are required for individuals to perform their work (voice, video, IM/chat, collaboration, email).

The following applies to the underlying systems that the UC EDS depends on and that are approved to collect PII:
The UC EDS obtains query results from IdSS which in turn depends on data collected by DEERS. DEERS is provided by the Defense Manpower Data Center (DMDC), who functions as the DoD Data Wholesaler for this data. These underlying systems collectively provide individuals the capability to review and update their data, such as the DMDC-provided Personnel Portal where users can review and update their data, enter or provide certain data, and be directed to other organizations and systems to update other data (such as in local DoD component Human Resources (HR) systems).

Individuals seeking to determine whether information about themselves is contained in this system of records

can submit written inquiries to Defense Information Systems Agency (DISA), Enterprise Services Directorate (ESD), 6919 Cooper Ave., Fort Meade, MD 20755-7901.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Display of contact data is required to implement and operate DoD communication systems. Contact data is made available so that individuals can communicate with each other in the variety of modes that are required for individuals to perform their work (voice, video, IM/chat, collaboration, email).

The following applies to the underlying systems that the UC EDS depends on and that are approved to collect PII:
The UC EDS obtains query results from IdSS which in turn depends on data collected by DEERS. DEERS is provided by the Defense Manpower Data Center (DMDC), who functions as the DoD Data Wholesaler for this data. These underlying systems collectively provide individuals the capability to review and update their data, such as the DMDC-provided Personnel Portal where users can review and update their data, enter or provide certain data, and be directed to other organizations and systems to update other data (such as in local DoD component Human Resources (HR) systems).

Individuals seeking to determine whether information about themselves is contained in this system of records can submit written inquiries to Defense Information Systems Agency (DISA), Enterprise Services Directorate (ESD), 6919 Cooper Ave., Fort Meade, MD 20755-7901.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☒ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

Item 2.k here is checked affirmatively for "Privacy Act Statement" and "Privacy Advisory" in relation to to the underlying systems that the UC EDS depends on and that are approved to collect PII: DEERS is provided by the Defense Manpower Data Center (DMDC), who functions as the DoD Data Wholesaler for this data. DMDC data is typically provided directly by the user, or by DoD Component systems that collect data, such as DoD component Human Resources IT systems. Individuals are provided a Privacy Act Statement and Privacy Advisories at the point where they enter and update their data in accordance with standard procedures for these systems. In addition, Privacy Advisories are provided when users access DoD end-user devices which, in turn, are used to access the applications that use the IdSS to establish user accounts (Exchange, SharePoint, vOffice, etc).

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.